Ma31a Elementos de Álgebra	**26 de Noviembre, 2007**

Examen

Prof. Cátedra: M. Kiwi — *Prof. Auxiliar: R. Cortez*

Tiempo 4.0 hrs.

Sea q una potencia de un primo p. Sea $n = q^m - 1$, β un elemento primitivo de $\mathbb{F}_{q^m}$ y $\ell \in \mathbb{N} \setminus \{0\}$.

En lo que sigue identificaremos $P = (p_0, \ldots, p_{n-1}) \in \mathbb{F}_q^n$, $P(x) = p_0 + p_1 x + \ldots + p_{n-1}x^{n-1} \in \mathbb{F}_q[x]$ y $[P] \in \mathbb{F}_q[x]/(x^n - 1)$.

Se dice que $\mathcal{C}$ es un código $\mathrm{BCH}_{\beta,\ell}$ primitivo de largo de bloque n sobre $\mathbb{F}_q$ y distancia de diseño $\delta \in \{2, \ldots, n\}$ si $\mathcal{C}$ es el ideal generado por $G(x)$ en $\mathbb{F}_q[x]/(x^n - 1)$ donde $G(x)$ es el mínimo común múltiplo de los polinomios minimales en $\mathbb{F}_p[x]$ de $\beta^\ell, \beta^{\ell+1}, \ldots, \beta^{\ell+\delta-2}$.

(i).- (0.5 pts) Sea $C \in \mathbb{F}_q^n$ y

$$H = \begin{pmatrix} 1 & \beta^\ell & \beta^{2\ell} & \ldots & \beta^{(n-1)\ell} \\ 1 & \beta^{\ell+1} & \beta^{2(\ell+1)} & \ldots & \beta^{(n-1)(\ell+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \beta^{\ell+\delta-2} & \beta^{2(\ell+\delta-2)} & \ldots & \beta^{(n-1)(\ell+\delta-2)} \end{pmatrix}.$$

Pruebe que $CH^T = 0$ si y sólo si $C(\beta^{\ell+j}) = 0$ para todo $j \in \{0, \ldots, \delta-2\}$.

(ii).- (0.75 pts) Pruebe que H es una matriz de paridad de $\mathcal{C}$, i.e. que $CH^T = 0$ si y sólo si $C \in \mathcal{C}$.

(iii).- (0.75 pts) Pruebe que el determinante de la submatriz de H conformada por sus columnas $i_1, i_2, \ldots, i_{\delta-1}$ es

$$\beta^{(i_1+i_2+\ldots+i_{\delta-1})\ell} \prod_{r<s} \left(\beta^{i_r} - \beta^{i_s}\right) \neq 0\,.$$

(iv).- (0.5 pts) Concluya que $\mathcal{C}$ es un código de distancia mínima al menos δ, i.e.

$$\min_{C \in \mathcal{C}, C \neq \vec{0}} |\{i : c_i \neq 0\}| \;\geq\; \delta\,.$$

(v).- (0.5 pts) Considere la realización de $\mathbb{F}_{2^3}$ dada por $\mathbb{F}_2[x]/(P)$ donde $P(x) = x^3 + x + 1$ y β raíz de P. Verifique que β es elemento primitivo de $\mathbb{F}_{2^3}$.

(vi).- (0.5 pts) Considere la realización de $\mathbb{F}_{2^3}$ y β como en la parte anterior. Como $\mathbb{F}_{2^3}$ es un espacio vectorial sobre $\mathbb{F}_2$, cada coordenada de la matriz H se puede ver como un vector en $\mathbb{F}_2^3$ sobre la base $\{1, \beta, \beta^2\}$ y H como una matriz de $3(\delta - 1) \times 7$. Para $\ell = 1$ y $\delta = 2$, construya la matriz de H asociada a $\mathrm{BCH}_{\beta,\ell}$. Asumiendo que hubo a lo más un error de transmision, indique a que palabra del código corresponde la palabra recibida 1101010.

En lo que sigue, sea $s \in \{0, \ldots, n-1\}$ y $C_s = \{p^t s \bmod n \,:\, t \in \mathbb{Z}\}$. Denotaremos $M^{(s)}(x) \in \mathbb{F}_p[x]$ al polinomio minimal de $\beta^s \in \mathbb{F}_{q^m}$.

(vii).- (0.75 pts) Pruebe que $M^{(ps)}(x) = M^{(s)}(x)$ y concluya que si $i \in C_s$, entonces $M^{(i)}(x)$ es divisible en $\mathbb{F}_q[x]$ por

$$\prod_{j \in C_s} \left(x - \beta^j\right) .$$

Indicación: Recuerde que en un cuerpo de característica p, elevar a la p es un transformación lineal.

(viii).- (1.0 pts) Pruebe que si s divide a r y $\alpha \in \mathbb{F}_{p^r}$, entonces $\alpha \in \mathbb{F}_{p^r}$ si y sólo si $\alpha^{p^s} = \alpha$. Concluya que

$$M^{(i)}(x) \;=\; \prod_{j \in C_s} \left(x - \beta^j\right) \in \mathbb{F}_p[x] .$$

Observe que $M^{(i)}(x)$ no depende del valor de $i \in C_s$.

(ix).- (0.75 pts) Considere la realización de $\mathbb{F}_{2^3}$ y β como en la la parte (iv). Determine para cada valor de $\delta \in \{2, \ldots, 7\}$ el polinomio generador $G \in \mathbb{F}_2[x]$ de un código $\mathrm{BCH}_{\beta,1}$ de largo de bloque 7 sobre $\mathbb{F}_2$ y distancia de diseño δ (indique cada uno de los coeficientes en $\mathbb{F}_2$ de G).